

REMARKS

Applicant appreciates the thorough examination of the present application as evidenced by the Office Action. Applicant submits that the present rejections should be withdrawn for the reasons discussed below.

The Prior Art Rejections

Claims 1-13, 16-34 and 37-44 stand rejected under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 6,028,860 to Laubach *et al.* ("Laubach"). The remaining claims stand rejected under Section 103 as unpatentable over Laubach in view of United States Patent No. 6,130,623 to MacLellan *et al.* Applicant notes that Laubach does not qualify as a 102(b) reference but has a 102(e) date prior to the filing date of the present application. Under 35 U.S.C. § 102, "a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (quoting *Verdegaal Bros. v. Union Oil Co.*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)). "The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" M.P.E.P. § 2112 (citations omitted) (emphasis added).

A finding of anticipation further requires that there must be no difference between the claimed invention and the disclosure of the cited reference as viewed by one of ordinary skill in the art. *See Scripps Clinic & Research Foundation v. Genentech Inc.*, 18 U.S.P.Q.2d 1001 (Fed. Cir. 1991). Thus, anticipation requires that a single prior art reference disclose each and every element of the anticipated claim.

Applicant respectfully submits that the independent claims are patentable at least because Laubach fails to disclose or suggest the use of encryption in connection with

communication of messages as recited in the independent claims. Applicant notes that Claims 1, 24 and 28 are directed to the encryption/transmission aspects of the invention while independent Claims 17, 26 and 38 are directed to the decryption/reception aspects. Accordingly, each group of independent claims will be addressed separately below.

Claim 1 recites:

A method of selective encryption of transmitted messages, comprising the steps of:
determining a group encryption key for an unencrypted message;
generating an error check value for the unencrypted message;
encrypting the unencrypted message using the group encryption key; and
transmitting the encrypted message and the error check value on a channel of a communication network with an associated destination address.

Thus, Claim 1 recites generating an error check value based on the unencrypted message and transmitting this unencrypted error check value with the encrypted message. The Office Action asserts with reference to independent Claim 1, and also independent Claims 24 and 28, that the "header error check (HEC)" of Laubach teaches the "error check value" of Claim 1. Office Action, p. 2. However, ~~the HEC of Laubach is not an error check~~ value for the unencrypted message as recited in Claim 1.

Laubach, unlike the present invention, relates to conventional multi-cast addressing of messages where stations are "assigned one or more station multicast addresses." Laubach, Col. 4, lines 6-7. Laubach describes a virtual connection protocol to "identify one or more subscriber terminal units (STUs) which are to receive the particular cell" based on "virtual path identifiers." Laubach, Col. 7, lines 23-32; Col. 8, lines 29-31. Thus, the distribution of multi-cast communications is based on an addressing protocol, not based on the encryption discussed in Laubach. Laubach, Col. 10, lines 39-44.

The ATM data of Laubach "refers to cells having a fixed length comprised of a header followed by a payload." Laubach, Col. 6, lines 30-31; Figures 11-12. ~~The HEC is for the unencrypted header of the ATM cell, not the encrypted payload.~~ Laubach, Col. 8, lines 55-61. It is clear from the receive side description in Laubach as well that only the payload, not the header, is encrypted. Laubach, Col. 9, lines 42-50. Thus, to analogize Laubach to Claim

1, the payload must correspond to the message that is encrypted. The HEC is not even based on the payload, nonetheless the payload after encryption. Accordingly, the rejection of independent Claim 1 and the claims that depend therefrom should be withdrawn for at least these reasons. The rejections of independent Claims 24 and 28 and the claims that depend therefrom should be withdrawn for substantially the same reasons based on corresponding recitations of those claims.

The Office Action also states "a HEC (or cyclical redundancy check, CRC) is generated for each individual unencrypted message (ATM cell) by a forward error correction processor." Office Action, p. 2. The CRC for forward error correction is based on the unencrypted header and the encrypted payload. Laubach, Col. 8, lines 60-66; Figure 4. Thus, the CRC (or FEC) is based on the encrypted payload, not the unencrypted payload. Accordingly, the FEC of Laubach also fails to disclose the error check value of independent Claims 1, 24, 28 and the claims that depend therefrom.

The distinctions between the present invention and Laubach are even more clear in the context of the decrypt/receive side claims. Claim 17 recites:

A method of selective decryption of transmitted messages, comprising the steps of:
receiving a message on a channel of a communication network;
determining if the received message is directed to a broadcast address of the communication network;
generating an error check value for the received message;
determining if the error check value indicates an error;
decrypting the received message using a group encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates an error;
generating an error check value for the decrypted message; and
assigning the received message to a group associated with the group encryption key if the error check value for the decrypted message indicates no error.

As with the encrypt/transmit claims discussed above, Claim 17 recites decrypting a message before generating the error check value. Accordingly, the rejection of Claim 17 and the claims that depend therefrom should be withdrawn for substantially the same reasons as discussed above with reference to Claim 1. The rejection of independent Claims 26, 38 and

the claims that depend therefrom should be withdrawn for similar reasons.

In addition, Claim 17 recites assigning a message to a group based on the group encryption key used to produce an error check value indicating no error. The Office Action states, without reference to a particular portion of Laubach, that a "decrypted message then can be sent (corresponding to the recited assigning or processing the message) to the intended computer(s) (corresponding to the recited group associated with the group encryption key)." Office Action, p. 4. As an initial matter, merely describing delivering a payload after decrypting does not disclose assigning a message to a group based on an error check value indicating no error. As discussed above, the assignment of a cell to a group for multi-cast purposes in Laubach is not based on encryption or decryption of the payload but is, instead, based on the virtual connections of Laubach. Laubach, Col. 10, lines 41-44. Accordingly, Applicant submits that independent Claims 17, 38 and the claims that depend therefrom should also be allowed for at least these additional reasons. Claims 9-12 should also be allowed for similar reasons.

Conclusion

Applicant respectfully submits that, for the reasons discussed above, the references cited in the present rejections do not disclose or suggest the present invention as claimed. Accordingly, Applicant respectfully requests allowance of all the pending claims and passing this application to issue.

Respectfully submitted,



Robert W. Glatz
Registration No. 36,811

Dated: February 2, 2004

Myers Bigel Sibley & Sajovec
P.O. Box 37428
Raleigh, NC 27627
(919) 854-1400 phone
(919) 854-1401 fax